Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Friday, January 20, 2006

Google challenges sweeping subpoena for search engine records

Not two days after I observed that the United States gives litigants intrusive discovery and subpoena powers, the Justice Department provides a good example. In pursuit of its case defending the Child Online Protection Act (COPA) in *ACLU v. Gonzales* that Department has commanded, via a subpoena for production of evidence, various search engines that are not parties to the suit (Google, Yahoo, etc.) to hand over very large samples of URLs available to be searched and search queries from you and me. For example, it commanded Google to hand over all "URL's" available to be searched "as of July 31, 2005" and and all queries performed on their search engines between June 1 and July 31st of 2005.

Fortunately, the subpoenas have not asked for information that might identify the querier (besides the query itself, which identifies all us "ego surfers" who like to keep track of what people are saying about us). Thus, it has not asked for your Internet protocol addresss that search engines could and probably routinely do record, or cookies which also can be used to tie together different searches that you have made.

Perhaps the DoJ is just looking to make a statistical study to justify the law, for example that some fraction of Internet searches are for porn. They may argue that if porn is available to a search engine, then it is effectively available to minors. According to Professor Orin Kerr, the DoJ is arguing that COPA requires password protection for pornography, not just filters: "DOJ's argument is that it needs the information from Google to explain the role of search engines in locating and obtaining pornography, which is then integral to understanding why filters are not an effective alternative to COPA screens [i.e., password protection]." However, unless the data is securely protected by the procedures (archaically designed for paper documents) specified in the protective order, the DoJ could use this data for a wide variety of surveillance unrelated to porn and COPA.

Here's a declaration that includes the subpoena, Google's response, and the protective order. Whereas MSN, AOL, and Yahoo complied with the subpoena (after apparently negotiating to reduce the amount of data), Google has objected to the subpoena. Good for Google! Powers to intrude on new kinds of privately collected data should never be given to a government without challenge, except where absolutely necessary in a truly urgent emergency, which this surely is not. (In other words, if this was September 12 and DoJ was asking airline web sites to hand over search queries for trips by plane to the East Coast the morning of the 11th, I'd expect Google to be patriotic and comply. Short of that kind of very rare and very urgent extremity, I expect and am happy to see them be patriotic and resist). If the Department of Justice wants Google's records, it will now have to ask the court to compel production under Federal Rules of Civil Procedure 45(c)(2)(B).

I hope the federal court allows the ACLU to examine that kind and volume of data in its discovery of the NSA. Much more likely is that

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

the Department of Justice is going to invoke national security to set up a very big double standard when it comes to discovery. The NSA can argue that protective orders designed for paper are woefully inadequate for protecting top secret digital data. Alas, they'd be right, even if it were just commercial trade secret data. Our law firms need and our courts should require 21st century security techniques for protection of discovered or subpoenaed digital evidence. We could, for example, use key splitting techniques and require that discovery be done on tamper-evident court computers with the evidence owner and a court official present. We might also in the future use multiparty secure computation for studies of the kind the DOJ, the ACLU, the FISA court, and so on would like to perform on sensitive digital data.

Given federal discovery rules, PATRIOT, FISA, and the unchecked and infinite power claimed by the executive branch, the sad fact as things stand now is that the feds claim the right to snoop on us almost at will. Indeed, the Justice Department is currently arguing that they have a perfect right to snoop on any aspect of our lives, whether we consider said aspect to be private or not, at will, if at their sole discretion they believe it is relevant to national security. But despite the supposed even-handedness of federal discovery rules, the federal government is going to declare that, when they get sensitive about it, we have very little right to check up on them. Since when do "public servants" get to conduct surveillance on "we the people" and not vice versa?

Posted by Nick Szabo at 5:21 PM

1 comment:

Jerome Carter said...

Since the "public servants" became our public masters, that's when.

8:01 AM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ▼ 2006 (130)
  - ► December (4)
  - ► November (7)
  - ► October (15)
  - ► September (15)
  - ► August (20)
  - ► July (5)
  - ► June (10)
  - ► May (4)
  - ► April (3)
  - ► March (11)
  - ► February (10)
  - ▼ January (26)
    - Death by government
    - Two views of Tiananmen Square
    - Free banker to be on Federal Reserve Board?
    - E-gold challenges forfeiture
    - History, property, and security -- update
    - BlackBerry appeal denied
    - Estimating the value of favors
    - Long distance trade in pre-Roman northern Europe

From contracts to money

Google challenges sweeping subpoena for search eng...

What data is on your hotel card key?

Some recent patent news

Professionals sue to stop illegal NSA surveillance...

Trial by ordeal

Laws for the mind police

Multiparty secure computation

More from former NSA spy

Warrantless NSA spying illegal -- more scholars an...

NSA spy doffs his mask

Cowen on currency

Schneier on Project Shamrock

"History and the Security of Property"

E-gold woes

"Imaginary" property

Defensible positions

Shells

► 2005 (44)

Simple theme. Powered by Blogger.